# Exhibit 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF ILLINOIS

| | |
|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and LYNAE VAHLE, individually, and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>ACKERCAMPS.COM LLC,<br><br>Defendant. | Case No. 1:22-cv-2256<br><br>CLASS ACTION |

I, Michael J. Roman, declare as follows:

1. I am over the age of 18. I am over the age of 18 and competent to testify to the facts and statements set forth in this declaration, and I testify to them from personal knowledge. If called as a witness, I would testify consistently with this declaration.

2. I am an associate attorney at Lewis Brisbois Bisgaard & Smith LLP, counsel for Defendant Ackercamps.com LLC ("Defendant") in this action.

2. Attached as **Exhibit A** is a true and accurate copy of the process, pleadings, and papers served upon Defendant on September 1, 2022 in this action. To date, Defendant has not been served process of a Summons and copy of Plaintiffs' Complaint.

3. Attached as **Exhibit B** is a true and accurate copy of the docket report from the Clerk of the Circuit Court of the First Judicial Circuit, Williamson County, Illinois for the cause styled *K.V., by and through her Guardian, Lynae Vahle, and Lynae Vahle v. Ackercamps.com LLC*, Case No. 2022-LA-108 (Cir. Ct. Williamson County).

4. Attached as **Exhibit C** is a true and accurate copy of all filings from the First Judicial Circuit, Williamson County, Illinois for the cause styled *K.V., by and through her Guardian, Lynae Vahle, and Lynae Vahle v. Ackercamps.com, LLC*, Case No. 2022-LA-108 (Cir. Ct. Williamson County).

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on September 30, 2022 in Chicago, Cook County, Illinois.

Michael J. Roman

FILED
Williamson Co. Circuit Court
1st Judicial Circuit
Date: 8/29/2022 10:02 AM
Justin Maze

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,

*Plaintiff*,

v.

ACKERCAMPS.COM LLC,

*Defendant.*

Case No.: 2022LA108

Judge:

**PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND REQUEST FOR DISCOVERY ON CERTIFICATION ISSUES**

In this case, Plaintiffs K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, (hereinafter "Plaintiffs"), alleges that Defendant Ackercamps.com LLC ("Defendant") systematically violated the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*. This case is well suited for class certification pursuant to 735 ILCS 5/2-801. Specifically, Plaintiffs seek to certify a class consisting of several hundred or more individuals who had their biometrics collected, captured, and/or stored by Defendant in the State of Illinois during the applicable statutory period in violation of BIPA. The question of liability is a legal question that can be answered in one fell swoop. As Plaintiffs' claims and the claims of similarly-situated individuals all arise from Defendant's uniform policies and practices, they satisfy the requirement of 735 ILCS 5/2-801 and should be certified. Notably, to Plaintiffs' Counsels' knowledge, the only BIPA class certification decisions issued to date have granted class certification. See, *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535 (N.D. Cal. 2018) (granting class certification) *aff'd Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019); and Ex. A, Mem. and Order, *Roberson v. Symphony Post Acute Care Network, et al.*, 17-L-733 (St. Clair County) (same).

**EXHIBIT A**

Plaintiffs move for class certification to protect members of the proposed class, individuals whose proprietary and legally protected personal and private biometric data was invaded by Defendant. Plaintiffs believe that the evidence and argumentation submitted with this motion are sufficient to allow the class to be certified now. However, in the event the Court (or Defendant) wishes for the parties to undertake formal discovery prior to the Court's consideration of this motion, Plaintiffs request that the Court allow Plaintiffs to supplement their briefing and defer the response and reply deadlines.

## I. RELEVANT BACKGROUND

### A. The Biometric Information Privacy Act

Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became wary of this then-growing, yet unregulated, technology. *See* 740 ILCS 14/5.

The Biometric Information Privacy Act, 740 ILCS 14/1, *et seq*. was enacted in 2008, arising from concerns that these experimental uses of finger-scan technologies created a "very serious need of protections for the citizens of Illinois when it comes to biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. Under the Act, it is unlawful for a private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless it first:

> (1) Informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;

> (2) Informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) Receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS 14/15(b).

Although there may be benefits with using biometrics, there are also serious risks. Unlike ID badges – which can be changed or replaced if stolen or compromised – biometrics, including face scans, are unique, permanent biometric identifiers associated with each individual. These biometrics are biologically unique to the individual; once compromised, the individual has ***no*** means by which to prevent identity theft, unauthorized tracking, or other unlawful or improper use of this information. This exposes individuals to serious and irreversible privacy risks. For example, if a biometric database is hacked, breached, or otherwise exposed – as in the Equifax, Uber, or thousands of other data breaches – individuals have no means to prevent the misappropriation and theft of their proprietary biometric makeup. Thus, recognizing the need to protect its citizens from harms like these, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

**B. Factual Allegations**

Plaintiffs filed this class action against Defendant on August 29, 2022, to redress Defendant's unlawful collection, use, storage, and disclosure of biometric information of Illinois citizens under BIPA. In their Class Action Complaint, Plaintiffs provided allegations that Defendant has and continues to violate BIPA through the collection of face-based biometrics without: (1) informing individuals in writing of the purpose and length of time for which face scan(s) were being collected,



**EXHIBIT A**

stored and used; (2) providing a publicly available retention schedule or guidelines for permanent destruction of the data; and (3) obtaining a written release, as required by BIPA.

Accordingly, Defendant's practices violated BIPA. As a result of Defendant's violations, Plaintiffs and similarly-situated individuals were subject to Defendant's uniform policies and practices and were victims of its scheme to unlawfully collect, store, and use individuals' biometric data in direct violation of BIPA.

Plaintiffs now seek class certification for the following similarly-situated individuals, defined as:

> All persons who had their biometric identifiers, facial geometry, faceprints, or facial data captured, collected, or received by Defendant while residing in Illinois from five years preceding the date of filing of this action through the date a class is certified in this action.

*Id.* at ¶ 70.

Given Defendant's standard practices defined above and the straightforward and common legal questions presented in this case, Plaintiffs now move for class certification. Notably, this motion is being filed shortly after the Complaint was filed and before the Defendant has responded. For the reasons discussed herein, Plaintiffs' request should be granted.

## II. STANDARD FOR CLASS CERTIFICATION

"The basic purpose of a class action is the efficiency and economy of litigation." *CE Design Ltd. v. C & T Pizza, Inc.*, 2015 IL App. (1st) 131465, ¶ 9 (Ill. App. Ct. May 8, 2015) (citing *Miner v. Gillette Co.*, 87 Ill. 2d 7, 14 (1981)). "In determining whether to certify a proposed class, the trial court accepts the allegations of the complaint as true and should err in favor of maintaining class certification." *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez v. Midway Moving & Storage, Inc.*, 378 Ill. App. 3d 51, 53 (2007)). Under Section 2-801 of the Code of Civil Procedure, a class may be certified if the following four requirements are met:

(1) the class is so numerous that a joinder of all members is impracticable;

(2) there are questions of fact or law common to the class that predominate over any questions affecting only individual members;

(3) the representative parties will fairly and adequately protect the interest of the class; and

(4) the class action is an appropriate method for the fair and efficient adjudication of the controversy.

*See Smith v. Illinois Cent. R.R. Co.*, 223 Ill. 2d 441, 447 (2006) (citing 735 ILCS 5/2-801). Notably, "[a] trial court has broad discretion in determining whether a proposed class meets the requirements for class certification." *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez*, 378 Ill. App. 3d at 53). Here, the allegations and facts in this case amply demonstrate that the four certification factors are met.

## III. ARGUMENT

Plaintiffs' claims here are especially suited for class certification because Defendant treated all class members identically for the purposes of applying BIPA. All of the putative class members in this case were uniformly subjected to the same illegal and unlawful collection, storage, and use of their biometric data by Defendant throughout the class period. Plaintiffs meet each of the statutory requirements for maintenance of this suit as a class action. Thus, the class action device is ideally suited and is far superior to burdening the Court with many individual lawsuits to address the same issues, undertake the same discovery, and rely on the same testimony.

### A. The Class Is So Numerous That Joinder of All Members Is Impracticable.

Numerosity is not dependent on plaintiff setting forth a precise number of class members or a listing of their names. *See Cruz v. Unilock Chicago*, 383 Ill. App. 3d 752, 771 (2d Dist. 2008) ("Of course, plaintiff need not demonstrate a precise figure for the class size, because a good-faith, nonspeculative estimate will suffice; rather, plaintiff need demonstrate only that the class is sufficiently numerous to make joinder of all of the members impracticable.") (internal citations omitted); *Hayna*

*v. Arby's, Inc.*, 99 Ill. App. 3d 700, 710-11 (1st Dist. 1981) ("It is not necessary that the class representative name the specific individuals who are possibly members of the class."). Courts in Illinois generally find numerosity when the class is comprised of at least 40 members. *See Wood River Area Dev. Corp. v. Germania Fed. Sav. Loan Ass'n*, 198 Ill. App. 3d 445, 450 (5th Dist. 1990).

In the present case, there can be no serious dispute that Plaintiffs meet the numerosity requirement. The class of potential plaintiffs is sufficiently large to make joinder impracticable. As result of Defendant's violations of BIPA, Plaintiffs and all similar-situated individuals were subject to Defendant's uniform policies and practices and were victims of Defendant's schemes to unlawfully collect, store and use their extremely personal and private biometric data in direct violation of BIPA. The precise number in the class cannot be determined until discovery records are obtained from Defendant. Nevertheless, class membership can be easily determined by reviewing Defendant's records. A review of Defendant's files regarding the collection, storage and use of biometric data performed during the class period is all that is needed to determine membership in Plaintiffs' proposed classes. *See e.g., Chultem v. Ticor Title Ins. Co.*, 401 Ill. App. 3d 226, 233 (1st Dist. 2010) (reversing Circuit Court's denial of class certification and holding that class was certifiable over defendants' objection that "the proposed class was not ascertainable, because the process of reviewing defendants' transaction files to determine class membership would be burdensome"); *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 539-40 (6th Cir. 2012)[1] (rejecting the argument that manual review of files should defeat certification agreeing with district court's reasoning that, if manual review was a bar, "defendants against whom claims of wrongful conduct have been made could escape class-wide review

[1] "Section 2-801 is patterned after Rule 23 of the Federal Rules of Civil Procedure and, because of this close relationship between the state and federal provision, 'federal decisions interpreting Rule 23 are persuasive authority with regard to questions of class certification in Illinois.'" *Cruz*, 383 Ill. App. 3d at 761 (quoting *Avery v. State Farm Mutual Automobile Insurance Co.*, 216 Ill.2d 100, 125 (2005)).

due solely to the size of their businesses or the manner in which their business records were maintained," and citing numerous courts that are in agreement, including *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery"). Once Defendant's records are obtained, the Court will know the precise number of persons affected.

Absent certification of this class action, putative class members may never know that their legal rights have been violated and as a result may never obtain the redress to which they are entitled under BIPA. Illinois courts have noted that denial of class certification where members of the putative class have no knowledge of the lawsuit may be the "equivalent of closing the door of justice" on the victims. *Wood River Area Dev. Corp. v. Germania Fed. Sav. & Loan Assn.*, 198 Ill.App.3d 445, 452 (5th Dist. 1990). Further, recognizing the need to protect its citizens from harms such as identity theft, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information. A class action would help ensure that Plaintiffs and all other similarly-situated individuals have a means of redress against Defendant for its widespread violations of BIPA.

**B. Common Questions Of Law And Fact Exist That Predominate Over Any Questions Solely Affecting Individual Members Of The Class.**

Courts analyze commonality and predominance under Section 2-801 by identifying the substantive issues that will control the outcome of the case. *See Bemis v. Safeco Ins. Co. of Am.*, 407 Ill. App. 3d 1164, 1167 (5th Dist. 2011); *Cruz*, 383 Ill. App. 3d at 773. The question then becomes whether those issues will predominate and whether they are common to the class, meaning that "favorable adjudication of the claims of the named plaintiffs will establish a right of recovery in other class members." *Cruz*, 383 Ill. App. 3d at 773. As stated by the Court of Appeals, the question is will

"common . . . issues be the subject of the majority of the efforts of the litigants and the court[?]" *Bemis*, 407 Ill. App. 3d at 1168. The answer here is "yes."

At the heart of this litigation is the culpable conduct of the Defendant under BIPA. The issues are simple and straightforward legal questions that plainly lend themselves to class-wide resolution. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregarded Plaintiffs' and other similarly-situated individuals' statutorily-protected privacy rights and unlawfully collected, stored, and used their biometric data in direct violation of BIPA. Specifically, Defendant has violated BIPA because it failed to: (1) inform Plaintiffs or the putative class in writing of the specific purpose and length of time for which their biometrics were being collected, stored, and used, as required by BIPA; (2) provide a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and the putative class's biometrics, as required by BIPA; and (3) receive a written release from Plaintiffs or the putative class to collect, capture, or otherwise obtain their biometrics, as required by BIPA. Additionally, Defendant unlawfully profited from the use of Plaintiffs' and Class Members' biometrics. Defendant treated the entire proposed class in precisely the same manner, resulting in identical violations of BIPA. These common biometric-collection practices create common issues of law and fact. In fact, the legality of Defendant's collection, storage, and use of biometric data is the focus of this litigation.

Indeed, once this Court determines whether Defendant's practice of collecting, storing, and using individuals' biometric data without adhering to the specific requirements of BIPA constitutes violations thereof, liability for the claims of class members will be determined in one stroke. The material facts and issues of law are substantially the same for the members of the class, and therefore these common issues could be tried such that proof as to one claimant would be proof as to all members of the class. This alone establishes predominance. The only remaining questions will be whether Defendant's violations caused members of the class to suffer damages and the proper

measure of damages and injunctive relief, which in and of themselves are questions common to the class. Accordingly, a favorable adjudication of the Plaintiffs' claims in this case will establish a right of recovery to all other class members, and thus the commonality and predominance requirements weigh in favor of certification of the class.

### C. The Named Plaintiffs and Class Counsel Are Adequate Representatives of The Class.

When evaluating adequacy, courts look to whether the named plaintiff has the same interests as those of the class and whether he or she will fairly represent them. *See CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 16. In this case, Plaintiffs' interest arises from statute. The class representatives, K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, are members of the proposed class and will fairly and adequately protect the class's interests. Plaintiffs used Defendant's "online photo galleries with facial recognition" feature or appeared in any photos within Bunk1's system which functions by collecting, capturing, and using facial biometrics. Each time Plaintiffs were in Bunk1's camp photos in their online system, the Defendant unlawfully collected their biometrics. Plaintiffs were never made aware of any publicly available BIPA policy. Further, Plaintiffs were never provided the information required by BIPA from Defendant. Plaintiffs have never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics. Plaintiffs have never been informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendant will ever permanently delete their biometrics. Plaintiffs have never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain their facial scan or facial geometry biometrics. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein. Thus, Plaintiffs were victims of the same uniform policies and practices of Defendant as the individuals they seek to

represent and is not seeking any relief that is potentially antagonistic to other members of the class. What is more, Plaintiffs have the interests of those class members in mind, as demonstrated by their willingness to sue on a class-wide basis and step forward as the class representative, which subjects Plaintiffs to discovery. This qualifies Plaintiffs as conscientious representative plaintiffs and satisfies the adequacy of representation requirement.

Proposed Class Counsel, Diana E. Wise of Wise Law LLC, will also fairly and adequately represent the class. Proposed Class Counsel is a highly qualified and experienced attorney, with over ten years of practicing law in the State of Illinois. Thus, Proposed Class Counsel is adequate and has the ability and resources to manage this lawsuit.

### D. A Class Action Is The Appropriate Method For Fair And Efficient Adjudication Of This Controversy.

Finally, a class action is the most appropriate method for the fair and efficient adjudication of this controversy, rather than bringing individual suits which could result in inconsistent determinations and unjust results. "It is proper to allow a class action where a defendant is alleged to have acted wrongfully in the same basic manner toward an entire class." *P.J.'s Concrete Pumping Service, Inc. v. Nextel West Corporation*, 345 Ill. App. 3d 992, 1003 (2d Dist. 2004). "The purported class representative must establish that a successful adjudication of its individual claims will establish a right of recovery or resolve a central issue on behalf of the class members." *Id.*

Here, Plaintiffs' claim stems from Defendant's common and uniform policies and practices, resulting in common violations of BIPA for all members of the class. Thus, class certification will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning Defendant's practices. *Wenthold v. AT&T Technologies, Inc.*, 142 Ill. App. 3d 612 (1st Dist. 1986). Without a class, the Court would have to hear dozens of additional individual cases raising identical questions of liability. Moreover, class members are better served by pooling resources rather than attempting to litigate individually. *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶¶ 28-30

(certifying TCPA class where statutory damages were alleged and rejecting arguments that individual lawsuits would be superior). In the interests of justice and judicial efficiency, it is desirable to concentrate the litigation of all class members' claims in a single forum. For all of these reasons, the class action is the most appropriate mechanism to adjudicate the claims in this case.

### E. In The Event The Court Or Defendant Seeks More Factual Information Regarding This Motion, The Court Should Allow Supplemental And Deferred Briefing Following Discovery.

There is no meaningful need for discovery for the Court to certify a class in this matter; Defendant's practices and policies are uniform. If, however, the Court wishes for the Parties to engage in discovery, the Court should keep the instant motion pending during the discovery period, allow Plaintiffs a supplemental brief, and defer Defendant's response and Plaintiffs' reply. Plaintiffs are moving as early as possible for class certification in part to avoid the "buy-off problem," which occurs when a defendant seeks to settle with a class representative on individual terms in an effort to moot the class claims asserted by the class representative. Plaintiffs are also moving for class certification now because the class should be certified, and because no meaningful discovery is necessary to establish that fact. The instant motion is far more than a placeholder or barebones memorandum. Rather, Plaintiffs' full arguments are set forth based on the facts known at this extremely early stage of litigation. Should the Court wish for more detailed factual information, the briefing schedule should be extended.

## IV. Conclusion

For the reasons stated above, Plaintiffs respectfully request that the Court enter an Order: (1) certifying Plaintiffs' claims as a class action; (2) appointing Plaintiffs as Class Representatives; (3) appointing Diana E. Wise of Wise Law LLC as Class Counsel; and (4) authorizing court-facilitated notice of this class action to the class. In the alternative, if this Court should allow discovery, allow Plaintiffs to supplement this briefing, and defer response and reply briefs.

Date: August 29, 2022

Respectfully submitted,

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiffs and the Proposed Class*



**EXHIBIT A**

## CERTIFICATE OF SERVICE

I hereby certify that on this date, I filed the foregoing document with the clerk of the Court using the Illinois E-Filing System, which should further distribute a true and accurate copy of the foregoing to all counsel of record.

*/s/ Diana E. Wise*



**EXHIBIT A**

FILED
Williamson Co. Circuit Court
1st Judicial Circuit
Date: 8/29/2022 10:02 AM
Justin Maze

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

| | | |
|---|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, | ) | |
| *Plaintiff*, | ) | |
| v. | ) | Case No.: 2022LA108 |
| ACKERCAMPS.COM LLC, | ) | Judge: |
| *Defendant.* | ) | |

**CLASS ACTION COMPLAINT**

Plaintiffs K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, (hereinafter "Plaintiffs"), bring this Class Action Complaint individually and on behalf of all other similarly situated individuals against Defendant Ackercamps.com LLC (hereinafter "Ackercamps.com LLC" or "Defendant") to stop Defendant's unlawful collection, use, storage, and disclosure of Plaintiffs' and the proposed Class's sensitive, private, and personal biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys. Further, Plaintiffs allege as follows:

**PARTIES, JURISDICTION, AND VENUE**

1. Plaintiff K.V., a minor, is an individual citizen of the State of Illinois. K.V. brings this case by and through her guardian, Lynae Vahle, an individual citizen of the State of Illinois.

2. Plaintiff Lynae Vahle is an individual citizen of the State of Illinois.

3. Defendant Ackercamps.com LLC is a limited liability company doing business as Bunk1. Defendant Ackercamps.com LLC is a Delaware corporation with a principal place of business in New York.



**EXHIBIT A**

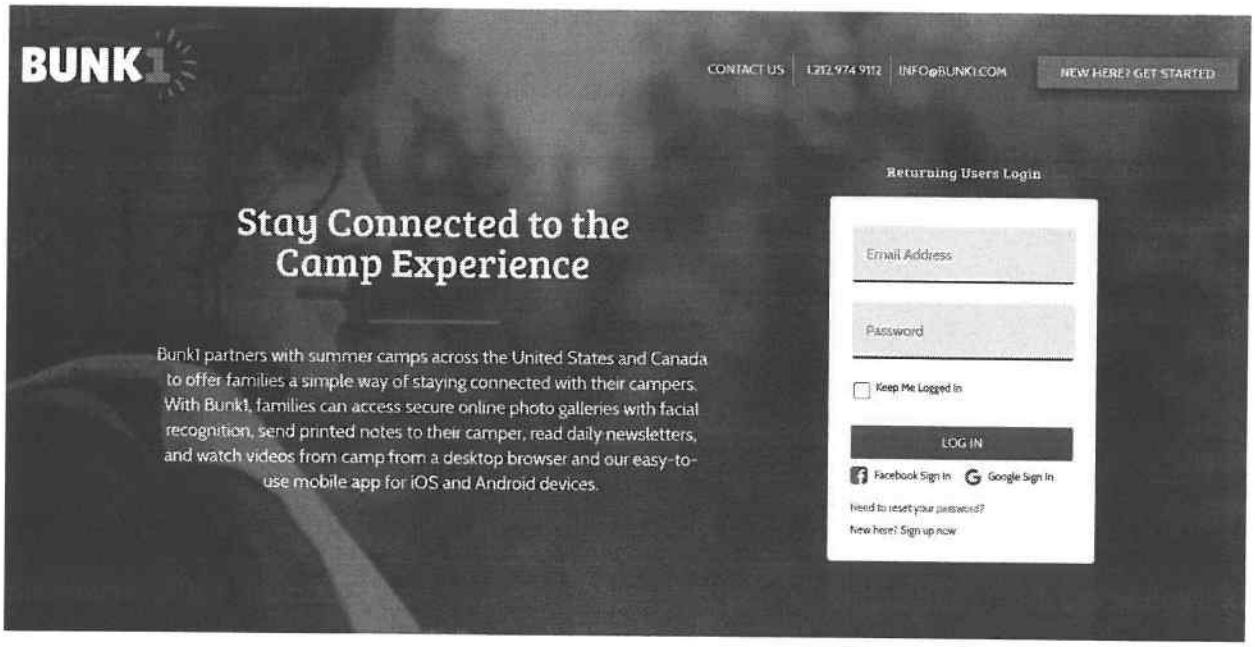
4. Defendant Ackercamps.com LLC may be served through its registered agent, Intertrust Corporate Services Delaware Ltd, 200 Bellevue Parkway, Suite 210, Wilmington, Delaware 19809.

5. Jurisdiction is proper in this Court as Plaintiffs are citizens of Illinois and Defendant targets business activity in Illinois, and purposefully avails itself of the laws, protections, and advantages of doing business in Illinois, with Illinois consumers like Plaintiffs.

6. Venue is proper in this court pursuant to 735 ILCS 5/2-101 as, upon information and belief, Defendant does business in this county.

## INTRODUCTION

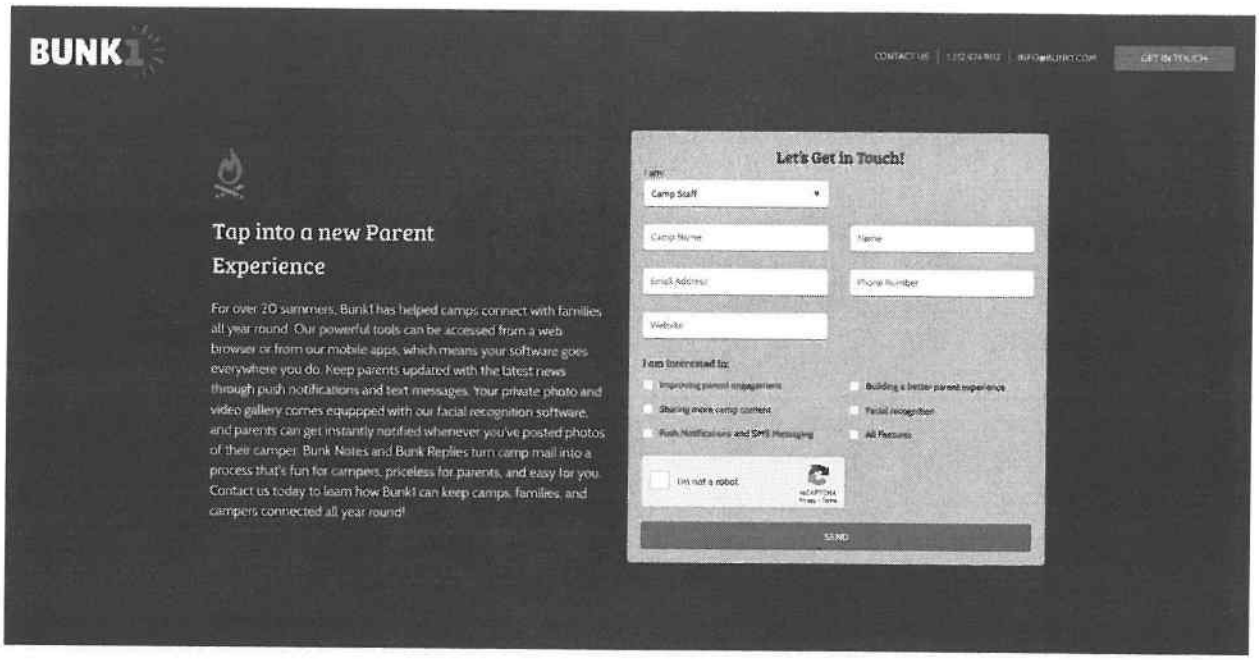
7. Defendant partners with summer camps across the United States to connect consumers with a specific person at a camp through access to online photo galleries with facial recognition.



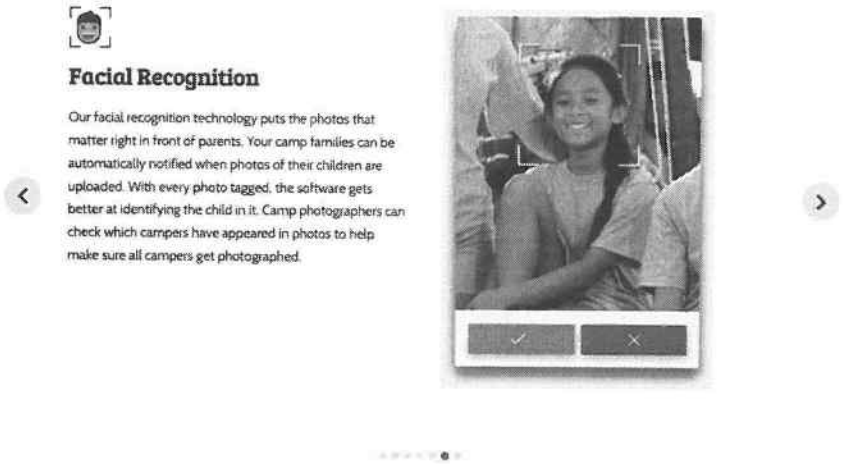

8. As part of its sales pitch, Defendant's camp photo and video gallery is equipped with "facial recognition software" that sends instant notification whenever a photo of a specific person is posted.



**EXHIBIT A**




**Boost Parent Engagement**




9. For Defendant's system to work, consumers must upload a high resolution, closeup "profile photo" of their specific person, so Defendant's facial recognition software can identify the specific person's facial geometry and detect possible matches within its online photo galleries.



**EXHIBIT A**

10. Defendant's "online photo galleries with facial recognition" functions, at least in part, by scanning, collecting, storing, and using customers' or potential customers' facial biometrics – including not only of campers, but also of any person in the photos, including potentially counselors, staff, siblings, parents, and friends.

11. This exposes Defendant's customers, potential customers, as well as any person in the camp's photos, including Plaintiffs, to serious and irreversible privacy risks.

12. For example, if a biometric database is hacked, breached, or otherwise exposed – such as in the recent Equifax data breach – consumers have ***no*** means by which to prevent identity theft, unauthorized tracking, and other improper or unlawful use of this information.

13. The Illinois Biometric Information Privacy Act (hereinafter "BIPA" or the "Act") expressly obligates Defendant to obtain an executed, written release from an individual, prior to the capture, collection, and/or storage of an individual's biometric identifiers or biometric information, especially a facial geometry scan, and biometric information derived from it. Burying a vague reference to biometric information in an online privacy policy is not sufficient to comply with BIPA's requirements.

14. BIPA further obligates Defendant to inform its potential customers in writing that a biometric identifier or biometric information is being collected or captured; to tell its potential customers in writing for how long it will store their biometric data or information and any purposes for which biometric information is being captured, collected, and used; and to make available a written policy disclosing when it will permanently destroy such information.

15. BIPA makes all of these requirements a *precondition* to the collection or recording of face geometry scans, or other associated biometric information. Under the Act, no biometric identifiers or biometric information may be captured, collected, purchased, or otherwise obtained if these pre-capture, pre-collection, pre-storage, or pre-obtainment requirements are not met.



**EXHIBIT A**

16. The State of Illinois takes the privacy of biometric data seriously.

17. There is no realistic way, absent surgery, to reassign someone's biometric data. A person can obtain a new social security number, but not a new face, which makes the protection of, and control over, biometric identifiers and biometric information critical.

18. Defendant captured, collected, received through trade, and/or otherwise obtained biometric identifiers or biometric information of their Illinois customers or potential customers, like Plaintiffs, without properly obtaining the above-described written executed release, and without making the required disclosures concerning the collection, storage, use, or destruction of biometric identifiers or information.

19. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and has not and will not destroy Plaintiffs' or the Class's biometric data as required by BIPA.

20. Plaintiffs and the putative Class are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the consumers' last interactions with the company.

21. Plaintiffs seek damages and injunctive relief for Defendant's BIPA violations, for themselves and all those similarly situated.

## PLAINTIFFS' SPECIFIC ALLEGATIONS

22. Plaintiffs have, at relevant times, had their biometrics – their facial geometry and associated information – collected, captured, and used by Defendant.

23. Plaintiffs either uploaded a "profile picture" to Bunk1 for Defendant's "online photo galleries with facial recognition" or appeared in any photos within Bunk1's system.

24. Defendant's "online photo galleries with facial recognition" functions by collecting, capturing, and using facial biometrics.

25. Upon information and belief, Defendant subsequently stored Plaintiffs' biometric data in its database(s).

26. After Plaintiffs either uploaded a "profile picture" to Bunk1 or appeared in any photo within Bunk1's system, Defendant unlawfully collected their biometrics.

27. Plaintiffs were never made aware of any publicly available BIPA policy. Further, Plaintiffs were never provided the information required by BIPA from Defendant.

28. Plaintiffs have never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics.

29. Plaintiffs have never been informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendant will ever permanently delete their biometrics.

30. Plaintiffs have never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain their facial scan or facial geometry biometrics.

31. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

32. BIPA protects consumers like Plaintiffs and the putative Class from this precise conduct, and Defendant had no right to secure this data.

33. Through BIPA, the Illinois legislature has created a right to receive certain information prior to a retailer securing their highly personal, private and proprietary biometric data. The legislature has chosen to define the capture of biometric data without receiving this extremely critical information as an injury.

34. Pursuant to 740 ILCS 14/15(b), Plaintiffs and the putative Class were entitled to receive certain information prior to Defendant securing their biometric data; namely, information advising them of the specific limited purpose(s) and length of time for which it/they collect(s), store(s),



**EXHIBIT A**

and use(s) their facial scans or facial geometry and any biometrics derived therefrom; information regarding Defendant's biometric retention policy; and, a written release allowing Defendant to collect and store their private biometric data.

## ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION

35. BIPA provides valuable privacy rights, protections, and benefits to consumers in Illinois.

36. For example, BIPA's requirements ensure that the environment for taking of biometrics is not forced or coerced; that individuals are freely advised that, by scanning one's facial geometry, the retailer is capturing, extracting, creating, and recording biometrics; that individuals can keep tabs on their biometric roadmaps *(e.g.,* who has their biometrics, for long how, and how it is being used), including after one's relationship ceases, or after the retailer stops storing the consumer's biometrics if at all; that individuals can evaluate the potential consequences of providing their biometrics; that companies must give individuals the right, and opportunity, to freely consent (or decline consent) **before taking** their biometrics; and that, if the disclosure does not say so, the consumer's biometrics will not be used for any other purpose except for those approved by the consumer. The BIPA-required environment for the taking of biometrics provides legislatively-imposed peace for biometric subjects.

37. To this end, in passing the Biometric Information Privacy Act (hereinafter "the Act") in 2008, the Illinois General Assembly found:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when

compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

...

(e) The full ramifications of biometric technology are not fully known.

(f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

See, 740 ILCS 14/5, Legislative findings; intent.

38. The law is specifically designed to require a company that collects biometrics to meet several conditions, **before collection**, aimed, in part, at educating and protecting the person whose biometrics it is taking for its own use, and requiring signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

39. The Act defines "Biometric identifier" as:

a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry...

See, 740 ILCS 14/10.

40. The Act defines "Biometric information" as:

any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

See, 740 ILCS 14/10.

41. The Act defines "Confidential and sensitive information" as:

personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.



**EXHIBIT A**

See, 740 ILCS 14/10.

42. The Act defines "Private entity" as:

> any individual, partnership, corporation, limited liability company, association, or other group, however organized…

See, 740 ILCS 14/10.

43. The Act defines "Written release" as:

> informed written consent or, in the context of employment, a release executed by an employee as a condition of employment

See, 740 ILCS 14/10.

44. The Act requires:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a).

45. Additionally, the Act provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).



**EXHIBIT A**

46. Further, the Act provides:

> No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

47. The Act also provides:

> No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

48. Furthermore, the Act provides:

> A private entity in possession of a biometric identifier or biometric information shall:
>
> (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
>
> (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 ILCS 14/15(e).

49. BIPA provides statutory damages if a private entity takes an Illinois consumer's biometrics and invades the consumer's privacy by circumventing BIPA's preconditions and requirements.



**EXHIBIT A**

50. The Act explicitly provides a private right of action for violations of the Act, and provides that a prevailing party "may recover for each violation:"

> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
>
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
>
> (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
>
> (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILCS 14/20.

51. In fact, BIPA requires express written consent in order to capture or collect biometrics in the first place. These formalized protections enable consumers to freely consent to the taking of their biometrics, if they so choose, after receiving legislatively-required information.

52. Defendant violated these clear protections of the Act, and upon information and belief, continues to violate its Illinois consumers' biometric privacy rights.

**DEFENDANT'S BIOMETRIC FACIAL-SCANNING OF ILLINOIS CONSUMERS**

53. Defendant's "online photo galleries with facial recognition" functions, at least in part, by collecting, capturing, and using consumer's biometrics.

54. Defendant captured, collected, stored, and/or otherwise obtained consumers' biometrics, without following BIPA's mandates, as part of its "online photo galleries with facial recognition."

55. Moreover, Defendant caused these biometrics to be associated with consumers, along with other consumer information.

56. Defendant has not, on information and belief, properly informed consumers in writing that a biometric identifier or biometric information is being captured, obtained, collected or stored;



**EXHIBIT A**

informed consumers in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; or obtained consumers' proper written consent to the capture, collection, obtainment or storage of their biometric identifier and biometric information derived from it.

57. Defendant's "online photo galleries with facial recognition" system captured, collected, stored, and/or otherwise obtained Plaintiffs' biometric identifier and other biometric information regarding Plaintiffs.

58. Defendant did not at any time, on information and belief:

a. inform Plaintiffs in writing (or otherwise) that a biometric identifier and biometric information was being obtained, captured, collected, and/or stored, or

b. inform Plaintiffs in writing (or otherwise) of the specific purposes and length of term for which a biometric identifier or biometric information was being collected, captured, stored, and/or used, or

c. obtain, or attempt to obtain, Plaintiffs' executed written release to have Plaintiffs' biometric identifier and biometric information captured, collected, stored, or recorded.

59. Plaintiffs did not provide a written release to Defendant as required by BIPA for the capture, collection, storage, obtainment, and/or use of Plaintiffs' biometric identifiers and information.

60. Nor did Plaintiffs know or fully understand that Defendant was collecting, capturing, and/or storing biometrics when Plaintiffs were scanning Plaintiffs' face; nor did Plaintiffs know or could Plaintiffs know all of the uses or purposes for which Plaintiffs' biometrics were taken.

61. Upon information and belief, Defendant has not publicly disclosed its retention schedule and guidelines for permanently destroying consumer biometric identifiers and information, if such guidelines even exist.



**EXHIBIT A**

62. Defendant, on information and belief, has no written policy, made available to the public, that discloses its retention schedule and/or guidelines for retaining and then permanently destroying biometric identifiers and information that complies with the requirements of BIPA.

63. The Illinois Legislature passed BIPA in in the wake of the bankruptcy of a company called Pay By Touch, which before its demise ran "the largest fingerprint scan system in Illinois." IL H.R. Tran. 2008 Reg. Sess. No. 276 at 249 (May 30, 2008). The bankruptcy, according to the Act's cosponsor, left "thousands of customers ... wondering what will become of their biometric ... data." *Id.*

64. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers or information, and/or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long.

65. The Pay by Touch bankruptcy highlights why conduct such as Defendant's – where individuals may be aware that they are providing biometric identifiers and information, but not aware of to whom or for what other purposes they are doing so – is dangerous.

66. Thus, BIPA is the Illinois Legislatures expression that Illinois citizens have biometric privacy rights, that BIPA is intended to protect.

67. Defendant disregarded these obligations and instead unlawfully collected, stored, and used consumers' biometric identifiers and information, without ever receiving the individual's informed written consent as required by BIPA.

68. Because Defendant neither published a BIPA-mandated data retention policy nor disclosed the purposes for their collection of biometric identifiers and information, Plaintiffs and the putative Class have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data.



**EXHIBIT A**

69. Likewise, Plaintiffs and the putative Class are not aware of how long Defendant will continue to store their biometric identifiers and information.

70. Nor are Plaintiffs and the putative Class told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a buyout, merger, or a bankruptcy.

71. By and through the actions detailed above, Defendant has not only disregard the Class' privacy rights, but it has also violated BIPA.

## CLASS ALLEGATIONS

72. Plaintiffs bring this action on behalf of themselves and pursuant to 735 ILCS 5/2-801 on behalf of a class (hereinafter the "Class") defined as follows:

> All persons who had their biometric identifiers, facial geometry, faceprints, or facial data captured, collected, or received by Defendant while residing in Illinois from five years preceding the date of filing of this action through the date a class is certified in this action.

Excluded from the class are Defendant's officers and directors, Plaintiffs' counsel, and any member of the judiciary presiding over this action.

73. **Numerosity:** The exact number of class members is unknown and is not available to Plaintiffs at this time, but upon information and belief, there are in excess of forty potential class members, and individual joinder in this case is impracticable. Class members can easily be identified through Defendant's records.

74. **Common Questions:** There are several questions of law and fact common to the claims of Plaintiffs and the Class members, and those questions predominate over any questions that may affect individual Class members. Common questions include, but are not limited to, the following:

a. whether Defendant has a practice of capturing or collecting consumers' biometrics;

b. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying

biometric identifiers and information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendant, whichever occurs first;

c. whether Defendant obtained an executed written release from face-scanned consumers before capturing, collecting, or otherwise obtaining consumers biometrics;

d. whether Defendant obtained an executed written release from face-scanned consumers before capturing, collecting, converting, sharing, storing or using consumer biometrics;

e. whether Defendant provided a writing disclosing to consumers the specific purposes for which the biometrics are being collected, stored, and used;

f. whether Defendant provided a writing disclosing to face-scanned consumers the length of time for which the biometrics are being collected, stored, and used;

g. whether Defendant's conduct violates BIPA;

h. whether Defendant's conduct was negligent, reckless, or willful;

i. whether Plaintiffs and Class members are entitled to damages, and what is the proper measure of damages; and

j. whether Plaintiffs and Class members are entitled to injunctive relief.

75. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interest of the class and have retained competent counsel experienced in complex litigation and class action litigation. Plaintiffs have no interests antagonistic to those of the class, and Defendant has no defenses unique to Plaintiffs.

76. **Appropriateness:** Class proceedings are also superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. Even if Class members were able or willing to pursue individual litigation, a class action would still be preferable due to the fact that a multiplicity of individual actions would likely increase the expense and time of litigation given the complex legal and factual controversies presented in this Class Action Complaint. A class action, on the other hand, provides the benefits of fewer management difficulties, single adjudication, economy of scale, and comprehensive supervision before a single Court, and

would result in reduced time, effort and expense for all parties and the Court, and ultimately, the uniformity of decisions.

**COUNT I – FOR DAMAGES AGAINST DEFENDANT**
**VIOLATION OF 740 ILCS 14/1, *ET SEQ.* – THE BIOMETRIC INFORMATION PRIVACY ACT**
**INDIVIDUALLY AND ON BEHALF OF THE CLASS**

77. Plaintiffs, individually and on behalf of all others similarly situated, repeat, re-allege, and incorporate all preceding paragraphs as if fully set forth herein.

78. BIPA is a remedial statute designed to protect Illinois consumers, by requiring consent and disclosures associated with the handling of biometrics, particularly in the context of biometric technology. 740 ILCS 14/5(g), 14/10, and 14/15(b)(3).

79. The Illinois Legislature's recognition of the importance of the public policy and benefits underpinning BIPA's enactment, and the regulation of biometrics collection, is detailed in the text of the statute itself.

80. Further, the Illinois Supreme Court, in a unanimous decision made clear that "**Compliance should not be difficult.**" *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 37 (Jan. 25, 2019).

81. Additionally, the Illinois Supreme Court has made clear that the Illinois Legislature intended to "subject[] private entities who fail to follow the statute's requirements to **substantial potential liability**, including liquidated damages, injunctions, attorney fees, and litigation expenses **'for each violation' of the law** (*id.* § 20) whether or not actual damages, beyond violation of the law's provisions, can be shown." *Id.* at ¶ 36 (emphasis added).

82. "It is clear that the legislature intended for this provision to have substantial force." *Id.* at ¶ 37.

83. Defendant has been and continues to be a "private entity" in possession of Plaintiffs'



**EXHIBIT A**

and other consumers' biometrics, and it collected, captured, or otherwise obtained their biometric identifiers and biometric information within the meaning of the Act.

84. As more fully set forth above, at relevant times Defendant collected, captured, or otherwise obtained, Plaintiffs' and other consumers' biometric identifiers and biometric information based on those identifiers as defined by BIPA, 740 ILCS 14/10, through Defendant's "online photo galleries with facial recognition."

85. In violation of 740 ILCS 14/15(a), Defendant failed to make such a written policy publicly available to Plaintiffs and other class members.

86. In violation of 740 ILCS 14/15(b), Defendant has collected, captured, stored, and/or otherwise obtained Plaintiffs' and other class members' biometric identifiers and biometric information, without:

a. informing Plaintiffs and the Class (including, where applicable, their legal authorized representatives), in writing, that the biometric identifiers or biometric information were being obtained, collected, captured, and/or stored;

b. informing Plaintiffs and the Class (including, where applicable, their legal authorized representatives), in writing, of the specific purpose and length of term for which the biometric identifiers or biometric information were being collected, stored, and used; and

c. receiving a written release executed by Plaintiffs and/or Class members and executed by Plaintiffs and/or Class members.

87. Defendant took Plaintiffs' and other class members' face scans, and knowingly caused their biometrics to be captured, collected, stored, and/or otherwise obtained without making publicly available the required policy that explains, for example, any purposes for which the biometric identifiers and information were collected, a retention schedule, and guidelines for permanently destroying biometric identifiers and information.

88. As a result of Defendant's above-described acts and omissions, Defendant has invaded the privacy of Plaintiffs and the Class; it has unlawfully and coercively taken their biometrics; it has

failed to provide them with information required by BIPA; it has deprived them of benefits, rights, opportunities and decisions conferred and required by the Illinois legislature via BIPA; and it illegally captured, collected, recorded, possessed, converted, and/or stored their face scans, biometrics, and property.

89. In violation of 740 ILCS 14/15(c) Defendant unlawfully profited from Plaintiffs' and Class Members' biometric identifiers and biometric information, including through using said biometric identifiers and biometric information to aid in sales of Defendant's products.

90. Accordingly, Defendant has violated the BIPA, and Plaintiffs and the Class have been damaged and are entitled to damages available under the BIPA, including liquidated damages of $1,000 per negligent violation, $5,000 per willful or reckless violation, or actual damages, whichever is greater. 740 ILCS 14/20(1).

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually and on behalf of the Class of similarly situated individuals, prays for an Order as follows:

A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the Class as defined herein;

B. Designating and appointing Plaintiffs as representatives of the Class and Plaintiffs' undersigned counsel as Class Counsel;

C. Entering judgment in favor of Plaintiffs and the Class and against Defendant;

D. Awarding Plaintiffs and the Class members liquidated damages of $1,000 per negligent violation, $5,000 per willful or reckless violation, or actual damages, whichever is greater, for each violation of BIPA;

E. Awarding Plaintiffs and the Class members reasonable attorneys' fees and costs incurred in this litigation; and



**EXHIBIT A**

F. Granting all such other and further relief as the Court deems just and appropriate.

**COUNT II – FOR INJUNCTIVE RELIEF AGAINST DEFENDANT VIOLATION OF 740 ILCS 14/1, *ET SEQ.* – THE BIOMETRIC INFORMATION PRIVACY ACT**

91. Plaintiffs, individually and on behalf of all others similarly situated, repeat, re-allege, and incorporate all preceding paragraphs as if fully set forth herein.

92. BIPA provides for injunctive relief. 740 ILCS 14/20(4).

93. Plaintiffs and other Class members are entitled to an order requiring Defendant to make disclosures consistent with the Act and enjoining further unlawful conduct.

94. First, Plaintiffs seek an order requiring Defendant to publicly disclose a written policy establishing any specific purpose and length of term for which Plaintiffs and other consumers' biometrics have been collected, captured, stored, obtained, and/or used, as well as guidelines for permanently destroying such biometrics when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, as required by 740 ILCS 14/15(a).

95. Second, Plaintiffs seek an order requiring Defendant to disclose whether Defendant has retained Plaintiffs' and other consumers' biometrics in any fashion, and if, when, and how such biometrics were permanently destroyed, consistent with BIPA.

96. Third, Plaintiffs seek an order requiring Defendant going forward to obtain a written release from any individual, prior to the capture, collection, and/or storage of that individual's biometric identifiers or biometric information, especially a facial geometry scan, and biometric information derived from it

97. Fourth, due to the above-described facts, and Defendant's failure to make publicly available facts demonstrating BIPA compliance as BIPA requires, Defendant should be ordered to: (i) disclose if (and if, precisely how, and to whom) it has disseminated, sold, leased, traded, or otherwise



**EXHIBIT A**

profited from Plaintiffs and other face scanned consumers' biometrics, which is strictly prohibited under BIPA; and (ii) disclose the standard of care that it employed to store, transmit, and protect such biometrics, as provided under BIPA. 740 ILCS 14/15(c), (d), (e).

98. Fifth, Defendant should be enjoined from further BIPA non-compliance and should be ordered to remedy any BIPA compliance deficiencies forthwith.

99. Plaintiffs and other Class members' legal interests are adverse to Defendant's legal interests. There is a substantial controversy between Plaintiffs and Class members and Defendant warranting equitable relief so that Plaintiffs and the Class may obtain the protections that BIPA entitles them to receive.

100. Plaintiffs and the Class do not know what Defendant has done (or intends to do) with their biometrics. Absent injunctive relief, Defendant is likely to continue its BIPA non-compliance and Plaintiffs and other Class members will continue to be in the dark on the subject.

101. For the reasons set forth above, Plaintiffs are likely to succeed on the merits of Plaintiffs' claims.

102. BIPA establishes the importance, value, and sensitive nature of biometrics, along with the need to protect and control it; Plaintiffs are entitled to know what Defendant has done with it as set forth above, and to an affirmation and verification that it has been or will be permanently destroyed as required by 740 ILCS 14/15(a).

103. The gravity of the harm to Plaintiffs and the Class, absent equitable relief, outweighs any harm to Defendant if such relief is granted.

104. As a result, Plaintiffs request commensurate injunctive relief.

**WHEREFORE**, Plaintiffs, individually and on behalf of the class, prays for an Order as follows:



**EXHIBIT A**

A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the class defined herein;

B. Designating and appointing Plaintiffs as representative of the class and Plaintiffs' undersigned counsel as class counsel;

C. Entering judgment in favor of Plaintiffs and the class and against Defendant;

D. Awarding Plaintiffs and the class members all damages available to Plaintiffs and the class available under applicable law, including statutory or liquidated damages;

E. Providing commensurate injunctive relief for Plaintiffs and class members as set forth above;

F. Awarding Plaintiffs and the Class members reasonable attorneys' fees and costs incurred in this litigation; and

G. Granting all such other and further relief as the Court deems just and appropriate.

Date:

Respectfully submitted,

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiffs and the Proposed Class*



**EXHIBIT A**

FILED
Williamson Co. Circuit Court
1st Judicial Circuit
Date: 8/29/2022 10:02 AM
Justin Maze

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

| | | |
|---|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, | ) | |
| *Plaintiff*, | ) | |
| v. | ) | Case No.: 2022LA108 |
| ACKERCAMPS.COM LLC, | ) | Judge: |
| *Defendant.* | ) | |

**RULE 222(b) AFFIDAVIT**

Pursuant to Illinois Supreme Court Rule 222(b), Plaintiff advises that this matter seeks more than $50,000.00 in damages.

Dated: August 29, 2022

Respectfully Submitted:

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiff and the Proposed Class*



**EXHIBIT A**

# Williamson County, IL

**NOTICE:** By clicking the 'Search' button below, or otherwise using the Judici.com website

**2022LA108 ACKERCAMPS COM LLC**



| Date | Entry | Judge |
|---|---|---|
| Entered Under: V , K | | |
| 09/07/2022 | Payment of $310.00 applied on 08/29/2022. | UNASSIGNED |
| 09/01/2022 | Case mgt conf set for 11/29/2022 at 9:00 in courtroom 8.<br>Video court set for 11/29/2022 at 9:00 in courtroom 8.<br>Notice of Appearance emailed to WISE, DIANA.<br>Standing cmc order & zoom log in filed. | UNASSIGNED |
| 08/30/2022 | INITIAL FILE REVIEW BY COURT. MOTION TO SERTIFY NOTED. SET CASE ON THE NOVEMBER 2022 CMC DOCKET AND SEND NOTICE. | JAG |
| 08/29/2022 | Class Action Complaint filed by WISE, DIANA. | UNASSIGNED |
| 08/29/2022 | Rule 222b Affidavit filed by WISE, DIANA. | UNASSIGNED |
| 08/29/2022 | Pls Motion For Certification & Request For Discovery On Certifaction issues filed by WISE, DIANA. | UNASSIGNED |
| 08/29/2022 | Judge review set for 08/30/2022 at 8:55 in courtroom CH. | UNASSIGNED |



**EXHIBIT B**

FILED
Williamson Co. Circuit Court
1st Judicial Circuit
Date: 8/29/2022 10:02 AM
Justin Maze

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

| | | |
|---|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, | ) | |
| *Plaintiff*, | ) | |
| v. | ) | Case No.: 2022LA108 |
| ACKERCAMPS.COM LLC, | ) | Judge: |
| *Defendant.* | ) | |

**CLASS ACTION COMPLAINT**

Plaintiffs K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, (hereinafter "Plaintiffs"), bring this Class Action Complaint individually and on behalf of all other similarly situated individuals against Defendant Ackercamps.com LLC (hereinafter "Ackercamps.com LLC" or "Defendant") to stop Defendant's unlawful collection, use, storage, and disclosure of Plaintiffs' and the proposed Class's sensitive, private, and personal biometric data. Plaintiffs allege as follows upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by their attorneys. Further, Plaintiffs allege as follows:

**PARTIES, JURISDICTION, AND VENUE**

1. Plaintiff K.V., a minor, is an individual citizen of the State of Illinois. K.V. brings this case by and through her guardian, Lynae Vahle, an individual citizen of the State of Illinois.

2. Plaintiff Lynae Vahle is an individual citizen of the State of Illinois.

3. Defendant Ackercamps.com LLC is a limited liability company doing business as Bunk1. Defendant Ackercamps.com LLC is a Delaware corporation with a principal place of business in New York.



**EXHIBIT C**

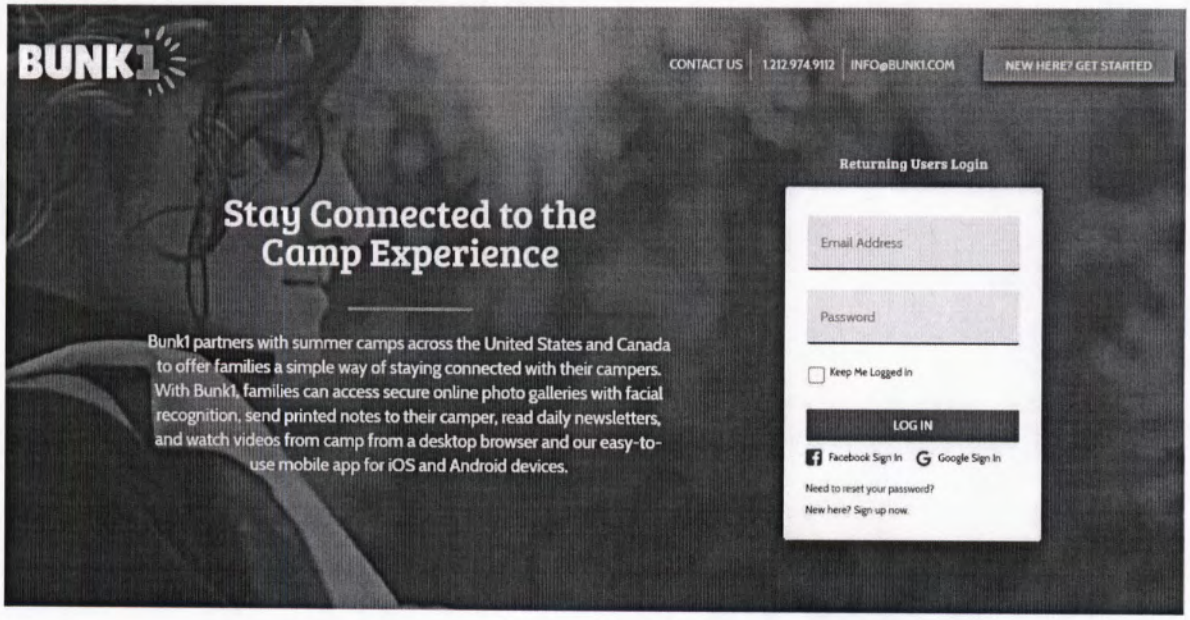
4. Defendant Ackercamps.com LLC may be served through its registered agent, Intertrust Corporate Services Delaware Ltd, 200 Bellevue Parkway, Suite 210, Wilmington, Delaware 19809.

5. Jurisdiction is proper in this Court as Plaintiffs are citizens of Illinois and Defendant targets business activity in Illinois, and purposefully avails itself of the laws, protections, and advantages of doing business in Illinois, with Illinois consumers like Plaintiffs.

6. Venue is proper in this court pursuant to 735 ILCS 5/2-101 as, upon information and belief, Defendant does business in this county.

## INTRODUCTION

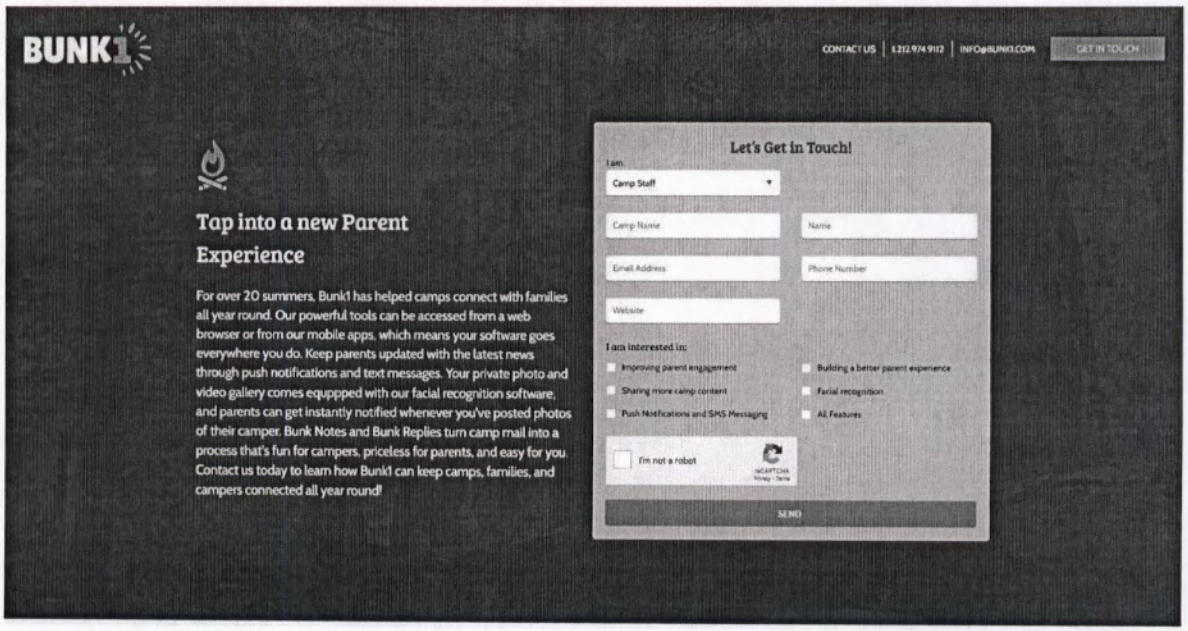
7. Defendant partners with summer camps across the United States to connect consumers with a specific person at a camp through access to online photo galleries with facial recognition.



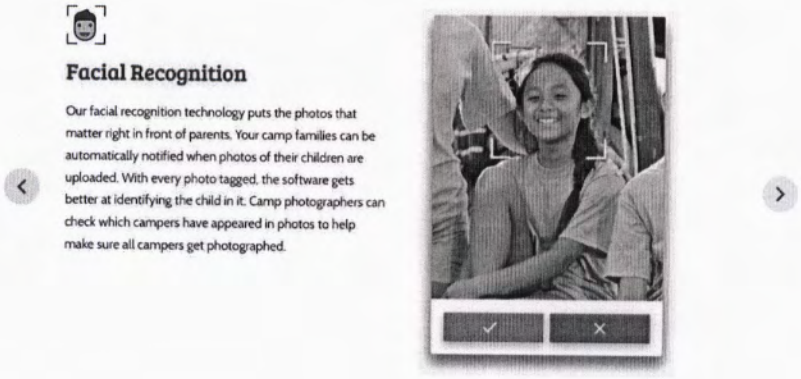

8. As part of its sales pitch, Defendant's camp photo and video gallery is equipped with "facial recognition software" that sends instant notification whenever a photo of a specific person is posted.



**EXHIBIT C**




**Boost Parent Engagement**




9. For Defendant's system to work, consumers must upload a high resolution, closeup "profile photo" of their specific person, so Defendant's facial recognition software can identify the specific person's facial geometry and detect possible matches within its online photo galleries.



**EXHIBIT C**

10. Defendant's "online photo galleries with facial recognition" functions, at least in part, by scanning, collecting, storing, and using customers' or potential customers' facial biometrics – including not only of campers, but also of any person in the photos, including potentially counselors, staff, siblings, parents, and friends.

11. This exposes Defendant's customers, potential customers, as well as any person in the camp's photos, including Plaintiffs, to serious and irreversible privacy risks.

12. For example, if a biometric database is hacked, breached, or otherwise exposed – such as in the recent Equifax data breach – consumers have [redacted] means by which to prevent identity theft, unauthorized tracking, and other improper or unlawful use of this information.

13. The Illinois Biometric Information Privacy Act (hereinafter "BIPA" or the "Act") expressly obligates Defendant to obtain an executed, written release from an individual, prior to the capture, collection, and/or storage of an individual's biometric identifiers or biometric information, especially a facial geometry scan, and biometric information derived from it. Burying a vague reference to biometric information in an online privacy policy is not sufficient to comply with BIPA's requirements.

14. BIPA further obligates Defendant to inform its potential customers in writing that a biometric identifier or biometric information is being collected or captured; to tell its potential customers in writing for how long it will store their biometric data or information and any purposes for which biometric information is being captured, collected, and used; and to make available a written policy disclosing when it will permanently destroy such information.

15. BIPA makes all of these requirements a *precondition* to the collection or recording of face geometry scans, or other associated biometric information. Under the Act, no biometric identifiers or biometric information may be captured, collected, purchased, or otherwise obtained if these pre-capture, pre-collection, pre-storage, or pre-obtainment requirements are not met.



**EXHIBIT C**

16. The State of Illinois takes the privacy of biometric data seriously.

17. There is no realistic way, absent surgery, to reassign someone's biometric data. A person can obtain a new social security number, but not a new face, which makes the protection of, and control over, biometric identifiers and biometric information critical.

18. Defendant captured, collected, received through trade, and/or otherwise obtained biometric identifiers or biometric information of their Illinois customers or potential customers, like Plaintiffs, without properly obtaining the above-described written executed release, and without making the required disclosures concerning the collection, storage, use, or destruction of biometric identifiers or information.

19. Upon information and belief, Defendant lacks retention schedules and guidelines for permanently destroying Plaintiffs' and the Class's biometric data and has not and will not destroy Plaintiffs' or the Class's biometric data as required by BIPA.

20. Plaintiffs and the putative Class are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the consumers' last interactions with the company.

21. Plaintiffs seek damages and injunctive relief for Defendant's BIPA violations, for themselves and all those similarly situated.

## PLAINTIFFS' SPECIFIC ALLEGATIONS

22. Plaintiffs have, at relevant times, had their biometrics – their facial geometry and associated information – collected, captured, and used by Defendant.

23. Plaintiffs either uploaded a "profile picture" to Bunk1 for Defendant's "online photo galleries with facial recognition" or appeared in any photos within Bunk1's system.

24. Defendant's "online photo galleries with facial recognition" functions by collecting, capturing, and using facial biometrics.

25. Upon information and belief, Defendant subsequently stored Plaintiffs' biometric data in its database(s).

26. After Plaintiffs either uploaded a "profile picture" to Bunk1 or appeared in any photo within Bunk1's system, Defendant unlawfully collected their biometrics.

27. Plaintiffs were never made aware of any publicly available BIPA policy. Further, Plaintiffs were never provided the information required by BIPA from Defendant.

28. Plaintiffs have never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics.

29. Plaintiffs have never been informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendant will ever permanently delete their biometrics.

30. Plaintiffs have never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain their facial scan or facial geometry biometrics.

31. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein.

32. BIPA protects consumers like Plaintiffs and the putative Class from this precise conduct, and Defendant had no right to secure this data.

33. Through BIPA, the Illinois legislature has created a right to receive certain information prior to a retailer securing their highly personal, private and proprietary biometric data. The legislature has chosen to define the capture of biometric data without receiving this extremely critical information as an injury.

34. Pursuant to 740 ILCS 14/15(b), Plaintiffs and the putative Class were entitled to receive certain information prior to Defendant securing their biometric data; namely, information advising them of the specific limited purpose(s) and length of time for which it/they collect(s), store(s),



**EXHIBIT C**

and use(s) their facial scans or facial geometry and any biometrics derived therefrom; information regarding Defendant's biometric retention policy; and, a written release allowing Defendant to collect and store their private biometric data.

**ILLINOIS'S STRONG STANCE ON PROTECTION OF BIOMETRIC INFORMATION**

35. BIPA provides valuable privacy rights, protections, and benefits to consumers in Illinois.

36. For example, BIPA's requirements ensure that the environment for taking of biometrics is not forced or coerced; that individuals are freely advised that, by scanning one's facial geometry, the retailer is capturing, extracting, creating, and recording biometrics; that individuals can keep tabs on their biometric roadmaps *(e.g.,* who has their biometrics, for long how, and how it is being used), including after one's relationship ceases, or after the retailer stops storing the consumer's biometrics if at all; that individuals can evaluate the potential consequences of providing their biometrics; that companies must give individuals the right, and opportunity, to freely consent (or decline consent) **before taking** their biometrics; and that, if the disclosure does not say so, the consumer's biometrics will not be used for any other purpose except for those approved by the consumer. The BIPA-required environment for the taking of biometrics provides legislatively-imposed peace for biometric subjects.

37. To this end, in passing the Biometric Information Privacy Act (hereinafter "the Act") in 2008, the Illinois General Assembly found:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when



**EXHIBIT C**

compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

...

(e) The full ramifications of biometric technology are not fully known.

(f) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

See, 740 ILCS 14/5, Legislative findings; intent.

38. The law is specifically designed to require a company that collects biometrics to meet several conditions, **before collection**, aimed, in part, at educating and protecting the person whose biometrics it is taking for its own use, and requiring signed, written consent attesting that the individual has been properly informed and has freely consented to biometrics collection.

39. The Act defines "Biometric identifier" as:

a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry...

See, 740 ILCS 14/10.

40. The Act defines "Biometric information" as:

any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

See, 740 ILCS 14/10.

41. The Act defines "Confidential and sensitive information" as:

personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.



**EXHIBIT C**

See, 740 ILCS 14/10.

42. The Act defines "Private entity" as:

> any individual, partnership, corporation, limited liability company, association, or other group, however organized…

See, 740 ILCS 14/10.

43. The Act defines "Written release" as:

> informed written consent or, in the context of employment, a release executed by an employee as a condition of employment

See, 740 ILCS 14/10.

44. The Act requires:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

740 ILCS 14/15(a).

45. Additionally, the Act provides:

> No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:
>
> (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;
>
> (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
>
> (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

740 ILCS 14/15(b).



**EXHIBIT C**

46. Further, the Act provides:

> No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

740 ILCS 14/15(c).

47. The Act also provides:

> No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
>
> (1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
>
> (2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
>
> (3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
>
> (4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

740 ILCS 14/15(d).

48. Furthermore, the Act provides:

> A private entity in possession of a biometric identifier or biometric information shall:
>
> (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
>
> (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

740 ILCS 14/15(e).

49. BIPA provides statutory damages if a private entity takes an Illinois consumer's biometrics and invades the consumer's privacy by circumventing BIPA's preconditions and requirements.



**EXHIBIT C**

50. The Act explicitly provides a private right of action for violations of the Act, and provides that a prevailing party "may recover for each violation:"

> (1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;
>
> (2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;
>
> (3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and
>
> (4) other relief, including an injunction, as the State or federal court may deem appropriate.

740 ILCS 14/20.

51. In fact, BIPA requires express written consent in order to capture or collect biometrics in the first place. These formalized protections enable consumers to freely consent to the taking of their biometrics, if they so choose, after receiving legislatively-required information.

52. Defendant violated these clear protections of the Act, and upon information and belief, continues to violate its Illinois consumers' biometric privacy rights.

**DEFENDANT'S BIOMETRIC FACIAL-SCANNING OF ILLINOIS CONSUMERS**

53. Defendant's "online photo galleries with facial recognition" functions, at least in part, by collecting, capturing, and using consumer's biometrics.

54. Defendant captured, collected, stored, and/or otherwise obtained consumers' biometrics, without following BIPA's mandates, as part of its "online photo galleries with facial recognition."

55. Moreover, Defendant caused these biometrics to be associated with consumers, along with other consumer information.

56. Defendant has not, on information and belief, properly informed consumers in writing that a biometric identifier or biometric information is being captured, obtained, collected or stored;



**EXHIBIT C**

informed consumers in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; or obtained consumers' proper written consent to the capture, collection, obtainment or storage of their biometric identifier and biometric information derived from it.

57. Defendant's "online photo galleries with facial recognition" system captured, collected, stored, and/or otherwise obtained Plaintiffs' biometric identifier and other biometric information regarding Plaintiffs.

58. Defendant did not at any time, on information and belief:

a. inform Plaintiffs in writing (or otherwise) that a biometric identifier and biometric information was being obtained, captured, collected, and/or stored, or

b. inform Plaintiffs in writing (or otherwise) of the specific purposes and length of term for which a biometric identifier or biometric information was being collected, captured, stored, and/or used, or

c. obtain, or attempt to obtain, Plaintiffs' executed written release to have Plaintiffs' biometric identifier and biometric information captured, collected, stored, or recorded.

59. Plaintiffs did not provide a written release to Defendant as required by BIPA for the capture, collection, storage, obtainment, and/or use of Plaintiffs' biometric identifiers and information.

60. Nor did Plaintiffs know or fully understand that Defendant was collecting, capturing, and/or storing biometrics when Plaintiffs were scanning Plaintiffs' face; nor did Plaintiffs know or could Plaintiffs know all of the uses or purposes for which Plaintiffs' biometrics were taken.

61. Upon information and belief, Defendant has not publicly disclosed its retention schedule and guidelines for permanently destroying consumer biometric identifiers and information, if such guidelines even exist.



**EXHIBIT C**

62. Defendant, on information and belief, has no written policy, made available to the public, that discloses its retention schedule and/or guidelines for retaining and then permanently destroying biometric identifiers and information that complies with the requirements of BIPA.

63. The Illinois Legislature passed BIPA in in the wake of the bankruptcy of a company called Pay By Touch, which before its demise ran "the largest fingerprint scan system in Illinois." IL H.R. Tran. 2008 Reg. Sess. No. 276 at 249 (May 30, 2008). The bankruptcy, according to the Act's cosponsor, left "thousands of customers ... wondering what will become of their biometric ... data." *Id.*

64. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers or information, and/or data derived therefrom, who exactly is collecting their biometric data, where it will be transmitted and for what purposes, and for how long.

65. The Pay by Touch bankruptcy highlights why conduct such as Defendant's – where individuals may be aware that they are providing biometric identifiers and information, but not aware of to whom or for what other purposes they are doing so – is dangerous.

66. Thus, BIPA is the Illinois Legislatures expression that Illinois citizens have biometric privacy rights, that BIPA is intended to protect.

67. Defendant disregarded these obligations and instead unlawfully collected, stored, and used consumers' biometric identifiers and information, without ever receiving the individual's informed written consent as required by BIPA.

68. Because Defendant neither published a BIPA-mandated data retention policy nor disclosed the purposes for their collection of biometric identifiers and information, Plaintiffs and the putative Class have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data.



**EXHIBIT C**

69. Likewise, Plaintiffs and the putative Class are not aware of how long Defendant will continue to store their biometric identifiers and information.

70. Nor are Plaintiffs and the putative Class told to whom Defendant currently discloses their biometric data, or what might happen to their biometric data in the event of a buyout, merger, or a bankruptcy.

71. By and through the actions detailed above, Defendant has not only disregard the Class' privacy rights, but it has also violated BIPA.

## CLASS ALLEGATIONS

72. Plaintiffs bring this action on behalf of themselves and pursuant to 735 ILCS 5/2-801 on behalf of a class (hereinafter the "Class") defined as follows:

> All persons who had their biometric identifiers, facial geometry, faceprints, or facial data captured, collected, or received by Defendant while residing in Illinois from five years preceding the date of filing of this action through the date a class is certified in this action.

Excluded from the class are Defendant's officers and directors, Plaintiffs' counsel, and any member of the judiciary presiding over this action.

73. **Numerosity:** The exact number of class members is unknown and is not available to Plaintiffs at this time, but upon information and belief, there are in excess of forty potential class members, and individual joinder in this case is impracticable. Class members can easily be identified through Defendant's records.

74. **Common Questions:** There are several questions of law and fact common to the claims of Plaintiffs and the Class members, and those questions predominate over any questions that may affect individual Class members. Common questions include, but are not limited to, the following:

a. whether Defendant has a practice of capturing or collecting consumers' biometrics;

b. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying



**EXHIBIT C**

biometric identifiers and information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of the individual's last interaction with Defendant, whichever occurs first;

c. whether Defendant obtained an executed written release from face-scanned consumers before capturing, collecting, or otherwise obtaining consumers biometrics;

d. whether Defendant obtained an executed written release from face-scanned consumers before capturing, collecting, converting, sharing, storing or using consumer biometrics;

e. whether Defendant provided a writing disclosing to consumers the specific purposes for which the biometrics are being collected, stored, and used;

f. whether Defendant provided a writing disclosing to face-scanned consumers the length of time for which the biometrics are being collected, stored, and used;

g. whether Defendant's conduct violates BIPA;

h. whether Defendant's conduct was negligent, reckless, or willful;

i. whether Plaintiffs and Class members are entitled to damages, and what is the proper measure of damages; and

j. whether Plaintiffs and Class members are entitled to injunctive relief.

75. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interest of the class and have retained competent counsel experienced in complex litigation and class action litigation. Plaintiffs have no interests antagonistic to those of the class, and Defendant has no defenses unique to Plaintiffs.

76. **Appropriateness:** Class proceedings are also superior to all other available methods for the fair and efficient adjudication of this controversy because joinder of all parties is impracticable. Even if Class members were able or willing to pursue individual litigation, a class action would still be preferable due to the fact that a multiplicity of individual actions would likely increase the expense and time of litigation given the complex legal and factual controversies presented in this Class Action Complaint. A class action, on the other hand, provides the benefits of fewer management difficulties, single adjudication, economy of scale, and comprehensive supervision before a single Court, and



**EXHIBIT C**

would result in reduced time, effort and expense for all parties and the Court, and ultimately, the uniformity of decisions.

**COUNT I – FOR DAMAGES AGAINST DEFENDANT**
**VIOLATION OF 740 ILCS 14/1, ET SEQ. – THE BIOMETRIC INFORMATION PRIVACY ACT**
**INDIVIDUALLY AND ON BEHALF OF THE CLASS**

77. Plaintiffs, individually and on behalf of all others similarly situated, repeat, re-allege, and incorporate all preceding paragraphs as if fully set forth herein.

78. BIPA is a remedial statute designed to protect Illinois consumers, by requiring consent and disclosures associated with the handling of biometrics, particularly in the context of biometric technology. 740 ILCS 14/5(g), 14/10, and 14/15(b)(3).

79. The Illinois Legislature's recognition of the importance of the public policy and benefits underpinning BIPA's enactment, and the regulation of biometrics collection, is detailed in the text of the statute itself.

80. Further, the Illinois Supreme Court, in a unanimous decision made clear that "**Compliance should not be difficult.**" *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, ¶ 37 (Jan. 25, 2019).

81. Additionally, the Illinois Supreme Court has made clear that the Illinois Legislature intended to "subject[] private entities who fail to follow the statute's requirements to **substantial potential liability**, including liquidated damages, injunctions, attorney fees, and litigation expenses **'for each violation' of the law** (*id.* § 20) whether or not actual damages, beyond violation of the law's provisions, can be shown." *Id.* at ¶ 36 (emphasis added).

82. "It is clear that the legislature intended for this provision to have substantial force." *Id.* at ¶ 37.

83. Defendant has been and continues to be a "private entity" in possession of Plaintiffs'



**EXHIBIT C**

and other consumers' biometrics, and it collected, captured, or otherwise obtained their biometric identifiers and biometric information within the meaning of the Act.

84. As more fully set forth above, at relevant times Defendant collected, captured, or otherwise obtained, Plaintiffs' and other consumers' biometric identifiers and biometric information based on those identifiers as defined by BIPA, 740 ILCS 14/10, through Defendant's "online photo galleries with facial recognition."

85. In violation of 740 ILCS 14/15(a), Defendant failed to make such a written policy publicly available to Plaintiffs and other class members.

86. In violation of 740 ILCS 14/15(b), Defendant has collected, captured, stored, and/or otherwise obtained Plaintiffs' and other class members' biometric identifiers and biometric information, without:

a. informing Plaintiffs and the Class (including, where applicable, their legal authorized representatives), in writing, that the biometric identifiers or biometric information were being obtained, collected, captured, and/or stored;

b. informing Plaintiffs and the Class (including, where applicable, their legal authorized representatives), in writing, of the specific purpose and length of term for which the biometric identifiers or biometric information were being collected, stored, and used; and

c. receiving a written release executed by Plaintiffs and/or Class members and executed by Plaintiffs and/or Class members.

87. Defendant took Plaintiffs' and other class members' face scans, and knowingly caused their biometrics to be captured, collected, stored, and/or otherwise obtained without making publicly available the required policy that explains, for example, any purposes for which the biometric identifiers and information were collected, a retention schedule, and guidelines for permanently destroying biometric identifiers and information.

88. As a result of Defendant's above-described acts and omissions, Defendant has invaded the privacy of Plaintiffs and the Class; it has unlawfully and coercively taken their biometrics; it has

failed to provide them with information required by BIPA; it has deprived them of benefits, rights, opportunities and decisions conferred and required by the Illinois legislature via BIPA; and it illegally captured, collected, recorded, possessed, converted, and/or stored their face scans, biometrics, and property.

89. In violation of 740 ILCS 14/15(c) Defendant unlawfully profited from Plaintiffs' and Class Members' biometric identifiers and biometric information, including through using said biometric identifiers and biometric information to aid in sales of Defendant's products.

90. Accordingly, Defendant has violated the BIPA, and Plaintiffs and the Class have been damaged and are entitled to damages available under the BIPA, including liquidated damages of $1,000 per negligent violation, $5,000 per willful or reckless violation, or actual damages, whichever is greater. 740 ILCS 14/20(1).

**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs, individually and on behalf of the Class of similarly situated individuals, prays for an Order as follows:

A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the Class as defined herein;

B. Designating and appointing Plaintiffs as representatives of the Class and Plaintiffs' undersigned counsel as Class Counsel;

C. Entering judgment in favor of Plaintiffs and the Class and against Defendant;

D. Awarding Plaintiffs and the Class members liquidated damages of $1,000 per negligent violation, $5,000 per willful or reckless violation, or actual damages, whichever is greater, for each violation of BIPA;

E. Awarding Plaintiffs and the Class members reasonable attorneys' fees and costs incurred in this litigation; and



**EXHIBIT C**

F. Granting all such other and further relief as the Court deems just and appropriate.

**COUNT II – FOR INJUNCTIVE RELIEF AGAINST DEFENDANT VIOLATION OF 740 ILCS 14/1, [redacted] – THE BIOMETRIC INFORMATION PRIVACY ACT**

91. Plaintiffs, individually and on behalf of all others similarly situated, repeat, re-allege, and incorporate all preceding paragraphs as if fully set forth herein.

92. BIPA provides for injunctive relief. 740 ILCS 14/20(4).

93. Plaintiffs and other Class members are entitled to an order requiring Defendant to make disclosures consistent with the Act and enjoining further unlawful conduct.

94. First, Plaintiffs seek an order requiring Defendant to publicly disclose a written policy establishing any specific purpose and length of term for which Plaintiffs and other consumers' biometrics have been collected, captured, stored, obtained, and/or used, as well as guidelines for permanently destroying such biometrics when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first, as required by 740 ILCS 14/15(a).

95. Second, Plaintiffs seek an order requiring Defendant to disclose whether Defendant has retained Plaintiffs' and other consumers' biometrics in any fashion, and if, when, and how such biometrics were permanently destroyed, consistent with BIPA.

96. Third, Plaintiffs seek an order requiring Defendant going forward to obtain a written release from any individual, prior to the capture, collection, and/or storage of that individual's biometric identifiers or biometric information, especially a facial geometry scan, and biometric information derived from it

97. Fourth, due to the above-described facts, and Defendant's failure to make publicly available facts demonstrating BIPA compliance as BIPA requires, Defendant should be ordered to: (i) disclose if (and if, precisely how, and to whom) it has disseminated, sold, leased, traded, or otherwise



**EXHIBIT C**

profited from Plaintiffs and other face scanned consumers' biometrics, which is strictly prohibited under BIPA; and (ii) disclose the standard of care that it employed to store, transmit, and protect such biometrics, as provided under BIPA. 740 ILCS 14/15(c), (d), (e).

98. Fifth, Defendant should be enjoined from further BIPA non-compliance and should be ordered to remedy any BIPA compliance deficiencies forthwith.

99. Plaintiffs and other Class members' legal interests are adverse to Defendant's legal interests. There is a substantial controversy between Plaintiffs and Class members and Defendant warranting equitable relief so that Plaintiffs and the Class may obtain the protections that BIPA entitles them to receive.

100. Plaintiffs and the Class do not know what Defendant has done (or intends to do) with their biometrics. Absent injunctive relief, Defendant is likely to continue its BIPA non-compliance and Plaintiffs and other Class members will continue to be in the dark on the subject.

101. For the reasons set forth above, Plaintiffs are likely to succeed on the merits of Plaintiffs' claims.

102. BIPA establishes the importance, value, and sensitive nature of biometrics, along with the need to protect and control it; Plaintiffs are entitled to know what Defendant has done with it as set forth above, and to an affirmation and verification that it has been or will be permanently destroyed as required by 740 ILCS 14/15(a).

103. The gravity of the harm to Plaintiffs and the Class, absent equitable relief, outweighs any harm to Defendant if such relief is granted.

104. As a result, Plaintiffs request commensurate injunctive relief.

**WHEREFORE**, Plaintiffs, individually and on behalf of the class, prays for an Order as follows:



**EXHIBIT C**

A. Finding this action satisfies the prerequisites for maintenance as a class action set forth in 735 ILCS 5/2-801, *et seq.*, and certifying the class defined herein;

B. Designating and appointing Plaintiffs as representative of the class and Plaintiffs' undersigned counsel as class counsel;

C. Entering judgment in favor of Plaintiffs and the class and against Defendant;

D. Awarding Plaintiffs and the class members all damages available to Plaintiffs and the class available under applicable law, including statutory or liquidated damages;

E. Providing commensurate injunctive relief for Plaintiffs and class members as set forth above;

F. Awarding Plaintiffs and the Class members reasonable attorneys' fees and costs incurred in this litigation; and

G. Granting all such other and further relief as the Court deems just and appropriate.

Date:

Respectfully submitted,

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiffs and the Proposed Class*



**EXHIBIT C**

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

| | | |
|---|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,<br><br>*Plaintiff*,<br><br>v.<br><br>ACKERCAMPS.COM LLC,<br><br>*Defendant.* | ) | Case No.: 2022LA108<br><br>Judge: |

**RULE 222(b) AFFIDAVIT**

Pursuant to Illinois Supreme Court Rule 222(b), Plaintiff advises that this matter seeks more than $50,000.00 in damages.

Dated: August 29, 2022

Respectfully Submitted:

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiff and the Proposed Class*



**EXHIBIT C**

**STATE OF ILLINOIS**
**IN THE CIRCUIT COURT OF THE FIRST JUDICIAL CIRCUIT**
**WILLIAMSON COUNTY**

| | | |
|---|---|---|
| K.V., a minor, by and through her Guardian, Lynae Vahle, and Lynae Vahle, individually, AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, | ) | |
| *Plaintiff*, | ) | |
| v. | ) | Case No.: 2022LA108 |
| ACKERCAMPS.COM LLC, | ) | Judge: |
| *Defendant.* | ) | |

**PLAINTIFFS' MOTION FOR CLASS CERTIFICATION AND REQUEST FOR DISCOVERY ON CERTIFICATION ISSUES**

In this case, Plaintiffs K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, (hereinafter "Plaintiffs"), alleges that Defendant Ackercamps.com LLC ("Defendant") systematically violated the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq*. This case is well suited for class certification pursuant to 735 ILCS 5/2-801. Specifically, Plaintiffs seek to certify a class consisting of several hundred or more individuals who had their biometrics collected, captured, and/or stored by Defendant in the State of Illinois during the applicable statutory period in violation of BIPA. The question of liability is a legal question that can be answered in one fell swoop. As Plaintiffs' claims and the claims of similarly-situated individuals all arise from Defendant's uniform policies and practices, they satisfy the requirement of 735 ILCS 5/2-801 and should be certified. Notably, to Plaintiffs' Counsels' knowledge, the only BIPA class certification decisions issued to date have granted class certification. See, *In re Facebook Biometric Info. Privacy Litig.*, 326 F.R.D. 535 (N.D. Cal. 2018) (granting class certification) *aff'd Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019); and Ex. A, Mem. and Order, *Roberson v. Symphony Post Acute Care Network, et al.*, 17-L-733 (St. Clair County) (same).

**EXHIBIT C**

Plaintiffs move for class certification to protect members of the proposed class, individuals whose proprietary and legally protected personal and private biometric data was invaded by Defendant. Plaintiffs believe that the evidence and argumentation submitted with this motion are sufficient to allow the class to be certified now. However, in the event the Court (or Defendant) wishes for the parties to undertake formal discovery prior to the Court's consideration of this motion, Plaintiffs request that the Court allow Plaintiffs to supplement their briefing and defer the response and reply deadlines.

## I. RELEVANT BACKGROUND

### A. The Biometric Information Privacy Act

Major national corporations started using Chicago and other locations in Illinois in the early 2000s to test "new [consumer] applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS 14/5(c). Given its relative infancy, an overwhelming portion of the public became wary of this then-growing, yet unregulated, technology. *See* 740 ILCS 14/5.

The Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* was enacted in 2008, arising from concerns that these experimental uses of finger-scan technologies created a "very serious need of protections for the citizens of Illinois when it comes to biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. Under the Act, it is unlawful for a private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless it first:

> (1) Informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored;



EXHIBIT C

(2) Informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) Receives a written release executed by the subject of the biometric identifier or biometric information."

740 ILCS 14/15(b).

Although there may be benefits with using biometrics, there are also serious risks. Unlike ID badges – which can be changed or replaced if stolen or compromised – biometrics, including face scans, are unique, permanent biometric identifiers associated with each individual. These biometrics are biologically unique to the individual; once compromised, the individual has [redacted] means by which to prevent identity theft, unauthorized tracking, or other unlawful or improper use of this information. This exposes individuals to serious and irreversible privacy risks. For example, if a biometric database is hacked, breached, or otherwise exposed – as in the Equifax, Uber, or thousands of other data breaches – individuals have no means to prevent the misappropriation and theft of their proprietary biometric makeup. Thus, recognizing the need to protect its citizens from harms like these, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

**B. Factual Allegations**

Plaintiffs filed this class action against Defendant on August 29, 2022, to redress Defendant's unlawful collection, use, storage, and disclosure of biometric information of Illinois citizens under BIPA. In their Class Action Complaint, Plaintiffs provided allegations that Defendant has and continues to violate BIPA through the collection of face-based biometrics without: (1) informing individuals in writing of the purpose and length of time for which face scan(s) were being collected,



EXHIBIT C

stored and used; (2) providing a publicly available retention schedule or guidelines for permanent destruction of the data; and (3) obtaining a written release, as required by BIPA.

Accordingly, Defendant's practices violated BIPA. As a result of Defendant's violations, Plaintiffs and similarly-situated individuals were subject to Defendant's uniform policies and practices and were victims of its scheme to unlawfully collect, store, and use individuals' biometric data in direct violation of BIPA.

Plaintiffs now seek class certification for the following similarly-situated individuals, defined as:

> All persons who had their biometric identifiers, facial geometry, faceprints, or facial data captured, collected, or received by Defendant while residing in Illinois from five years preceding the date of filing of this action through the date a class is certified in this action.

*Id.* at ¶ 70.

Given Defendant's standard practices defined above and the straightforward and common legal questions presented in this case, Plaintiffs now move for class certification. Notably, this motion is being filed shortly after the Complaint was filed and before the Defendant has responded. For the reasons discussed herein, Plaintiffs' request should be granted.

## II. STANDARD FOR CLASS CERTIFICATION

"The basic purpose of a class action is the efficiency and economy of litigation." *CE Design Ltd. v. C & T Pizza, Inc.*, 2015 IL App. (1st) 131465, ¶ 9 (Ill. App. Ct. May 8, 2015) (citing *Miner v. Gillette Co.*, 87 Ill. 2d 7, 14 (1981)). "In determining whether to certify a proposed class, the trial court accepts the allegations of the complaint as true and should err in favor of maintaining class certification." *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez v. Midway Moving & Storage, Inc.*, 378 Ill. App. 3d 51, 53 (2007)). Under Section 2-801 of the Code of Civil Procedure, a class may be certified if the following four requirements are met:

(1) the class is so numerous that a joinder of all members is impracticable;

(2) there are questions of fact or law common to the class that predominate over any questions affecting only individual members;

(3) the representative parties will fairly and adequately protect the interest of the class; and

(4) the class action is an appropriate method for the fair and efficient adjudication of the controversy.

*See Smith v. Illinois Cent. R.R. Co.*, 223 Ill. 2d 441, 447 (2006) (citing 735 ILCS 5/2-801). Notably, "[a] trial court has broad discretion in determining whether a proposed class meets the requirements for class certification." *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 9 (citing *Ramirez*, 378 Ill. App. 3d at 53). Here, the allegations and facts in this case amply demonstrate that the four certification factors are met.

## III. ARGUMENT

Plaintiffs' claims here are especially suited for class certification because Defendant treated all class members identically for the purposes of applying BIPA. All of the putative class members in this case were uniformly subjected to the same illegal and unlawful collection, storage, and use of their biometric data by Defendant throughout the class period. Plaintiffs meet each of the statutory requirements for maintenance of this suit as a class action. Thus, the class action device is ideally suited and is far superior to burdening the Court with many individual lawsuits to address the same issues, undertake the same discovery, and rely on the same testimony.

### A. The Class Is So Numerous That Joinder of All Members Is Impracticable.

Numerosity is not dependent on plaintiff setting forth a precise number of class members or a listing of their names. *See Cruz v. Unilock Chicago*, 383 Ill. App. 3d 752, 771 (2d Dist. 2008) ("Of course, plaintiff need not demonstrate a precise figure for the class size, because a good-faith, nonspeculative estimate will suffice; rather, plaintiff need demonstrate only that the class is sufficiently numerous to make joinder of all of the members impracticable.") (internal citations omitted); *Hayna*



EXHIBIT C

*v. Arby's, Inc.*, 99 Ill. App. 3d 700, 710-11 (1st Dist. 1981) ("It is not necessary that the class representative name the specific individuals who are possibly members of the class."). Courts in Illinois generally find numerosity when the class is comprised of at least 40 members. *See Wood River Area Dev. Corp. v. Germania Fed. Sav. Loan Ass'n*, 198 Ill. App. 3d 445, 450 (5th Dist. 1990).

In the present case, there can be no serious dispute that Plaintiffs meet the numerosity requirement. The class of potential plaintiffs is sufficiently large to make joinder impracticable. As result of Defendant's violations of BIPA, Plaintiffs and all similar-situated individuals were subject to Defendant's uniform policies and practices and were victims of Defendant's schemes to unlawfully collect, store and use their extremely personal and private biometric data in direct violation of BIPA. The precise number in the class cannot be determined until discovery records are obtained from Defendant. Nevertheless, class membership can be easily determined by reviewing Defendant's records. A review of Defendant's files regarding the collection, storage and use of biometric data performed during the class period is all that is needed to determine membership in Plaintiffs' proposed classes. *See e.g., Chultem v. Ticor Title Ins. Co.*, 401 Ill. App. 3d 226, 233 (1st Dist. 2010) (reversing Circuit Court's denial of class certification and holding that class was certifiable over defendants' objection that "the proposed class was not ascertainable, because the process of reviewing defendants' transaction files to determine class membership would be burdensome"); *Young v. Nationwide Mut. Ins. Co.*, 693 F.3d 532, 539-40 (6th Cir. 2012)[1] (rejecting the argument that manual review of files should defeat certification agreeing with district court's reasoning that, if manual review was a bar, "defendants against whom claims of wrongful conduct have been made could escape class-wide review

[1] "Section 2-801 is patterned after Rule 23 of the Federal Rules of Civil Procedure and, because of this close relationship between the state and federal provision, 'federal decisions interpreting Rule 23 are persuasive authority with regard to questions of class certification in Illinois.'" *Cruz*, 383 Ill. App. 3d at 761 (quoting *Avery v. State Farm Mutual Automobile Insurance Co.*, 216 Ill.2d 100, 125 (2005)).



EXHIBIT C

due solely to the size of their businesses or the manner in which their business records were maintained," and citing numerous courts that are in agreement, including *Perez v. First Am. Title Ins. Co.*, 2009 WL 2486003, at *7 (D. Ariz. Aug. 12, 2009) ("Even if it takes a substantial amount of time to review files and determine who is eligible for the [denied] discount, that work can be done through discovery"). Once Defendant's records are obtained, the Court will know the precise number of persons affected.

Absent certification of this class action, putative class members may never know that their legal rights have been violated and as a result may never obtain the redress to which they are entitled under BIPA. Illinois courts have noted that denial of class certification where members of the putative class have no knowledge of the lawsuit may be the "equivalent of closing the door of justice" on the victims. *Wood River Area Dev. Corp. v. Germania Fed. Sav. & Loan Assn.*, 198 Ill.App.3d 445, 452 (5th Dist. 1990). Further, recognizing the need to protect its citizens from harms such as identity theft, Illinois enacted BIPA specifically to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information. A class action would help ensure that Plaintiffs and all other similarly-situated individuals have a means of redress against Defendant for its widespread violations of BIPA.

**B. Common Questions Of Law And Fact Exist That Predominate Over Any Questions Solely Affecting Individual Members Of The Class.**

Courts analyze commonality and predominance under Section 2-801 by identifying the substantive issues that will control the outcome of the case. *See Bemis v. Safeco Ins. Co. of Am.*, 407 Ill. App. 3d 1164, 1167 (5th Dist. 2011); *Cruz*, 383 Ill. App. 3d at 773. The question then becomes whether those issues will predominate and whether they are common to the class, meaning that "favorable adjudication of the claims of the named plaintiffs will establish a right of recovery in other class members." *Cruz*, 383 Ill. App. 3d at 773. As stated by the Court of Appeals, the question is will



EXHIBIT C

"common . . . issues be the subject of the majority of the efforts of the litigants and the court[?]" *Bemis*, 407 Ill. App. 3d at 1168. The answer here is "yes."

At the heart of this litigation is the culpable conduct of the Defendant under BIPA. The issues are simple and straightforward legal questions that plainly lend themselves to class-wide resolution. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregarded Plaintiffs' and other similarly-situated individuals' statutorily-protected privacy rights and unlawfully collected, stored, and used their biometric data in direct violation of BIPA. Specifically, Defendant has violated BIPA because it failed to: (1) inform Plaintiffs or the putative class in writing of the specific purpose and length of time for which their biometrics were being collected, stored, and used, as required by BIPA; (2) provide a publicly available retention schedule and guidelines for permanently destroying Plaintiffs' and the putative class's biometrics, as required by BIPA; and (3) receive a written release from Plaintiffs or the putative class to collect, capture, or otherwise obtain their biometrics, as required by BIPA. Additionally, Defendant unlawfully profited from the use of Plaintiffs' and Class Members' biometrics. Defendant treated the entire proposed class in precisely the same manner, resulting in identical violations of BIPA. These common biometric-collection practices create common issues of law and fact. In fact, the legality of Defendant's collection, storage, and use of biometric data is the focus of this litigation.

Indeed, once this Court determines whether Defendant's practice of collecting, storing, and using individuals' biometric data without adhering to the specific requirements of BIPA constitutes violations thereof, liability for the claims of class members will be determined in one stroke. The material facts and issues of law are substantially the same for the members of the class, and therefore these common issues could be tried such that proof as to one claimant would be proof as to all members of the class. This alone establishes predominance. The only remaining questions will be whether Defendant's violations caused members of the class to suffer damages and the proper

measure of damages and injunctive relief, which in and of themselves are questions common to the class. Accordingly, a favorable adjudication of the Plaintiffs' claims in this case will establish a right of recovery to all other class members, and thus the commonality and predominance requirements weigh in favor of certification of the class.

### C. The Named Plaintiffs and Class Counsel Are Adequate Representatives of The Class.

When evaluating adequacy, courts look to whether the named plaintiff has the same interests as those of the class and whether he or she will fairly represent them. *See CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶ 16. In this case, Plaintiffs' interest arises from statute. The class representatives, K.V., a minor, by and through her guardian, Lynae Vahle, and Lynae Vahle, individually, are members of the proposed class and will fairly and adequately protect the class's interests. Plaintiffs used Defendant's "online photo galleries with facial recognition" feature or appeared in any photos within Bunk1's system which functions by collecting, capturing, and using facial biometrics. Each time Plaintiffs were in Bunk1's camp photos in their online system, the Defendant unlawfully collected their biometrics. Plaintiffs were never made aware of any publicly available BIPA policy. Further, Plaintiffs were never provided the information required by BIPA from Defendant. Plaintiffs have never been informed of the specific limited purposes or length of time for which Defendant collected, stored, or used their biometrics. Plaintiffs have never been informed of any biometric data retention policy developed by Defendant, nor have they ever been informed of whether Defendant will ever permanently delete their biometrics. Plaintiffs have never been provided with nor ever signed a written release allowing Defendant to collect, capture, store, or otherwise obtain their facial scan or facial geometry biometrics. Plaintiffs have continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA alleged herein. Thus, Plaintiffs were victims of the same uniform policies and practices of Defendant as the individuals they seek to

represent and is not seeking any relief that is potentially antagonistic to other members of the class. What is more, Plaintiffs have the interests of those class members in mind, as demonstrated by their willingness to sue on a class-wide basis and step forward as the class representative, which subjects Plaintiffs to discovery. This qualifies Plaintiffs as conscientious representative plaintiffs and satisfies the adequacy of representation requirement.

Proposed Class Counsel, Diana E. Wise of Wise Law LLC, will also fairly and adequately represent the class. Proposed Class Counsel is a highly qualified and experienced attorney, with over ten years of practicing law in the State of Illinois. Thus, Proposed Class Counsel is adequate and has the ability and resources to manage this lawsuit.

**D. A Class Action Is The Appropriate Method For Fair And Efficient Adjudication Of This Controversy.**

Finally, a class action is the most appropriate method for the fair and efficient adjudication of this controversy, rather than bringing individual suits which could result in inconsistent determinations and unjust results. "It is proper to allow a class action where a defendant is alleged to have acted wrongfully in the same basic manner toward an entire class." *P.J.'s Concrete Pumping Service, Inc. v. Nextel West Corporation*, 345 Ill. App. 3d 992, 1003 (2d Dist. 2004). "The purported class representative must establish that a successful adjudication of its individual claims will establish a right of recovery or resolve a central issue on behalf of the class members." *Id.*

Here, Plaintiffs' claim stems from Defendant's common and uniform policies and practices, resulting in common violations of BIPA for all members of the class. Thus, class certification will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning Defendant's practices. *Wenthold v. AT&T Technologies, Inc.*, 142 Ill. App. 3d 612 (1st Dist. 1986). Without a class, the Court would have to hear dozens of additional individual cases raising identical questions of liability. Moreover, class members are better served by pooling resources rather than attempting to litigate individually. *CE Design Ltd.*, 2015 IL App. (1st) 131465, ¶¶ 28-30

(certifying TCPA class where statutory damages were alleged and rejecting arguments that individual lawsuits would be superior). In the interests of justice and judicial efficiency, it is desirable to concentrate the litigation of all class members' claims in a single forum. For all of these reasons, the class action is the most appropriate mechanism to adjudicate the claims in this case.

### E. In The Event The Court Or Defendant Seeks More Factual Information Regarding This Motion, The Court Should Allow Supplemental And Deferred Briefing Following Discovery.

There is no meaningful need for discovery for the Court to certify a class in this matter; Defendant's practices and policies are uniform. If, however, the Court wishes for the Parties to engage in discovery, the Court should keep the instant motion pending during the discovery period, allow Plaintiffs a supplemental brief, and defer Defendant's response and Plaintiffs' reply. Plaintiffs are moving as early as possible for class certification in part to avoid the "buy-off problem," which occurs when a defendant seeks to settle with a class representative on individual terms in an effort to moot the class claims asserted by the class representative. Plaintiffs are also moving for class certification now because the class should be certified, and because no meaningful discovery is necessary to establish that fact. The instant motion is far more than a placeholder or barebones memorandum. Rather, Plaintiffs' full arguments are set forth based on the facts known at this extremely early stage of litigation. Should the Court wish for more detailed factual information, the briefing schedule should be extended.

## IV. Conclusion

For the reasons stated above, Plaintiffs respectfully request that the Court enter an Order: (1) certifying Plaintiffs' claims as a class action; (2) appointing Plaintiffs as Class Representatives; (3) appointing Diana E. Wise of Wise Law LLC as Class Counsel; and (4) authorizing court-facilitated notice of this class action to the class. In the alternative, if this Court should allow discovery, allow Plaintiffs to supplement this briefing, and defer response and reply briefs.



**EXHIBIT C**

Date: August 29, 2022

Respectfully submitted,

By: */s/ Diana E. Wise*
Diana E. Wise – IL Bar #6304459
WISE LAW LLC
1778 Caprice Court
O'Fallon, IL 62269
Ph: 217-556-8036
Email: dwise@wiseconsumerlaw.com

*Attorney for Plaintiffs and the Proposed Class*



**EXHIBIT C**

**CERTIFICATE OF SERVICE**

I hereby certify that on this date, I filed the foregoing document with the clerk of the Court using the Illinois E-Filing System, which should further distribute a true and accurate copy of the foregoing to all counsel of record.

*/s/ Diana E. Wise*



**EXHIBIT C**